

BLUETOOTHTM 1.1

**Connect
Without
Cables**

SECOND EDITION

Bluetooth 1.1's ◀
dramatic improvements in
interoperability and reliability

Includes thoroughly revised ◀
coverage of Bluetooth security
and power conservation

New Bluetooth profiles— ◀
*including the long-awaited
Personal Area Networking profile!*

**Jennifer Bray and
Charles F Sturman**

Foreword by Tom Siep, General Manager of Bluetooth SIG, Inc.

Contents

Foreword to the Second Edition	xvii
Foreword to the First Edition	xix
Preface to the Second Edition	xxi
Preface to the First Edition	xxiii
Acknowledgments	xxv
Introduction	xxvii
1 Overview	1
1.1 Bluetooth's Origins	2
1.2 The Bluetooth SIG	2
1.3 Aims	4
1.4 The Protocol Stack	5
1.5 Security	12

1.6	Applications and Profiles	12
1.7	Using Bluetooth	13
1.8	Management	17
1.9	Test and Qualification	18
1.10	Bluetooth in Context	19
1.11	Summary	22

Protocol Stack Part 1—The Bluetooth Module

2	Antennas	25
2.1	Radiation Pattern	25
2.2	Gains and Losses	27
2.3	Types of Antennas	28
2.4	Ceramic Antennas	30
2.5	On-chip Antennas	30
2.6	Antenna Placement	31
2.7	Summary	31
3	Radio	32
3.1	Introduction	32
3.2	Frequency Hopping	33
3.3	Modulation	33
3.4	Symbol Timing	34
3.5	Power Emission and Control	34
3.6	Radio Performance Parameters	35
3.7	Simple RF Architecture	36
3.8	RF System Timing	39
3.9	Blue RF	39
3.10	Summary	40
4	Baseband	41
4.1	Introduction	41
4.2	Bluetooth Device Address	42

Contents	vii
4.3 Masters, Slaves, and Piconets	42
4.4 System Timing	45
4.5 Physical Links: SCO and ACL	48
4.6 Bluetooth Packet Structure	49
4.7 Packet Types and Packet Construction	57
4.8 Logical Channels	58
4.9 Channel Coding and Bitstream Processing	59
4.10 Timebase Synchronisation and Receive Correlation	62
4.11 Frequency Hopping	63
4.12 Summary	64
5 The Link Controller	65
5.1 Introduction	65
5.2 Link Control Protocol	65
5.3 Link Controller States	67
5.4 Link Controller Operation	70
5.5 Piconet Operation	79
5.6 Scatternet Operation	82
5.7 Master / Slave Role Switching	84
5.8 Low-Power Operation	88
5.9 Baseband / Link Controller Architectural Overview	88
5.10 Summary	90
6 Audio	93
6.1 Introduction	93
6.2 Audio Transports in the Protocol Stack	94
6.3 Quality and Bandwidth	94
6.4 SCO Links	95
6.5 Audio CODECs	96
6.6 Audio Subsystem	99
6.7 Audio Data Formats and HCI	101
6.8 Implementation	102
6.9 Summary	102

7	The Link Manager	103
7.1	LMP Protocol Data Units (PDUs)	104
7.2	The Link Management Channel	104
7.3	Link Setup	105
7.4	LMP Link Shutdown	108
7.5	Role Change	109
7.6	Control of Multi-Slot Packets	111
7.7	Security	112
7.8	Low-Power Modes	112
7.9	Power Control	112
7.10	Quality of Service	114
7.11	<i>Information Messages</i>	114
7.12	Supported Features	114
7.13	LMP Version	115
7.14	Name Request	116
7.15	Test Mode	117
7.16	Summary	117
8	The Host Controller Interface	119
8.1	HCI Packet Types	121
8.2	The HCI Transport Layer	125
8.3	Flow Control	128
8.4	Configuring Modules	130
8.5	<i>Inquiring: Discovering Other Bluetooth Devices</i>	<i>134</i>
8.6	<i>Inquiry Scan: Becoming Discoverable</i>	<i>137</i>
8.7	<i>Paging: Initiating Connections</i>	<i>140</i>
8.8	<i>Page Scan: Receiving Connections</i>	<i>141</i>
8.9	<i>Sending and Receiving Data</i>	<i>145</i>
8.10	<i>Switching Roles</i>	<i>147</i>
8.11	<i>Power Control</i>	<i>147</i>
8.12	<i>Summary</i>	<i>148</i>

Protocol Stack Part 2—The Bluetooth Host

9	Logical Link Control and Adaptation Protocol	151
9.1	Multiplexing Using Channels	152
9.2	L2CAP Signalling	153
9.3	Establishing a Connection	156
9.4	Configuring a Connection	160
9.5	Transferring Data	162
9.6	Disconnecting and Timeouts	164
9.7	Connectionless Data Channels	166
9.8	Enabling and Disabling Incoming Connectionless Traffic	167
9.9	Handling Groups	168
9.10	Echo and Ping	170
9.11	Get Information	171
9.12	L2CAP State Machine	172
9.13	Implementation-Dependent Issues	173
9.14	Summary	175
10	RFCOMM	176
10.1	Serial Ports and UARTs	177
10.2	Types of RFCOMM Devices	177
10.3	RFCOMM Frame Types	178
10.4	Connecting and Disconnecting	179
10.5	Structure of RFCOMM Frames	180
10.6	Multiplexer Frames	186
10.7	Service Records	194
10.8	Summary	195
11	The Service Discovery Protocol	196
11.1	SDP Client/Server Model	197
11.2	The SDP Database	198
11.3	Browsing SDP Records	204

11.4	Universally Unique Identifiers (UUIDs)	205
11.5	SDP Messages	208
11.6	Service Discovery Profile	221
11.7	Summary	223
12	The Wireless Application Protocol	224
12.1	The WAP Forum	225
12.2	The WAP Stack	226
12.3	PPP Links	227
12.4	WAP Clients and Servers	231
12.5	Suspend and Resume	233
12.6	Service Discovery	234
12.7	WAP Interoperability	234
12.8	Using WAP	234
12.9	Summary	236
13	OBEX and IrDA	237
13.1	OBEX in the Bluetooth Stack	238
13.2	Object Model	240
13.3	Session Protocol	242
13.4	Summary	249
14	Telephony Control Protocol	251
14.1	TCS Signalling	253
14.2	Call Establishment Signalling	256
14.3	Call Clearing Signalling	262
14.4	DTMF Signalling	264
14.5	Wireless User Group (WUG) Signalling	265
14.6	Connectionless Signalling	269
14.7	TCS Call States	270
14.8	Summary	271

Protocol Stack Part 3—Cross Layer Functions

15	Encryption and Security	275
15.1	Key Generation and the Encryption Engine	277
15.2	Secret Keys and PINs	282
15.3	Pairing and Bonding	283
15.4	Starting Encryption	292
15.5	Security Modes	294
15.6	Security Architecture	295
15.7	Summary	298
16	Low-Power Operation	300
16.1	Controlling Low-Power Modes	301
16.2	Hold Mode	301
16.3	Sniff Mode	304
16.4	Park Mode	308
16.5	Low-Power Oscillator	318
16.6	Summary	318
17	Quality of Service	320
17.1	Requesting QOS	323
17.2	QOS Violations	328
17.3	Flushing and Delays	329
17.4	Link Supervision	331
17.5	Broadcast Channel Reliability	332
17.6	Data Rates and Packet Types	333
17.7	Summary	338
18	Managing Bluetooth Devices	339
18.1	Link Configuration and Management	340
18.2	Device Manager Architecture	351

18.3	Security Management	355
18.4	Integrating Applications	356
18.5	Accounting Management	357
18.6	Capacity	358
18.7	User Interface Design	358
18.8	Summary	360

Applications—The Bluetooth Profiles

19 Foundation Profiles

19.1	Structure of Profiles	365
19.2	The Generic Access Profile	365
19.3	The Serial Port Profile	367
19.4	Dial Up Networking	369
19.5	FAX Profile	372
19.6	Headset Profile	373
19.7	LAN Access Point Profile	375
19.8	Generic Object Exchange Profile	378
19.9	Object Push Profile	379
19.10	File Transfer Profile	380
19.11	Synchronisation Profile	381
19.12	Intercom Profile	382
19.13	The Cordless Telephony Profile	383
19.14	Benefits of Profiles	385
19.15	Summary	386

20 Draft Post – Foundation Profiles 388

20.1	The Human Interface Device Profile	389
20.2	The Hands-Free Profile	397
20.3	The Basic Imaging Profile	405
20.4	The Basic Printing Profile	415
20.5	The Hard Copy Cable Replacement Profile	423
20.6	Summary	427

21	Personal Area Networking	428
21.1	The PAN Profile	428
21.2	Bluetooth Network Encapsulation Profile	435
21.3	Summary	443
22	ESDP for UPnP	444
22.1	Universal Plug and Play Device Architecture	444
22.2	L2CAP Based Solutions	447
22.3	IP Based Solutions	449
22.4	Summary	451

Test and Qualification

23	Test Mode	455
23.1	Activating Test Mode	455
23.2	Controlling Test Mode	458
23.3	Radio Transmitter Test	460
23.4	Loopback Test	463
23.5	Summary	464
24	Qualification and Type Approval	465
24.1	Bluetooth Qualification	466
24.2	Bluetooth Interoperability Testing	474
24.3	Regulatory Type Approval	475
24.4	Summary	476

Bluetooth in Context

25	Implementation	479
25.1	Introduction	479
25.2	System Partitioning	480
25.3	Hardware Integration Options	488
25.4	Bluetooth as an IP Core	492

25.5	ASIC Prototyping and FPGAs	497
25.6	Making the Right Design Choices	497
25.7	Radio Implementation	499
25.8	Summary	501
26	Related Standards and Technologies	502
26.1	Introduction	502
26.2	What Are the Requirements?	502
26.3	Infrared Data Association (IrDA)	503
26.4	Digital Enhanced Cordless Telecommunications (DECT)	504
26.5	IEEE 802.11	506
26.6	The HomeRF™ Working Group (HRFWG)	509
26.7	IEEE 802.15 and the Wireless Personal Area Network (WPAN)	511
26.8	HIPERLAN	512
26.9	MMAC	514
26.10	The Future	514
26.11	Summary	516
26.12	Useful Web Addresses	517
27	The Bluetooth Market	518
27.1	Introduction	518
27.2	Market Pull and Technology Push	518
27.3	Market Segments	521
27.4	Success in the Marketplace	523
27.5	Enabling Technologies and Components	525
27.6	Consumer Products	526
27.7	The Bluetooth Brand	527
27.8	Summary	529
28	Future Developments	530
28.1	Working Groups and New Bluetooth Profiles	531
28.2	Profile Working Groups	532
28.3	Future Bluetooth Core Specifications	535
28.4	Summary	537

Contents	xv
Appendix—Bluetooth 1.1 Updates	538
Glossary	550
References	577
Index	581